CYBERWEAPONS: POWER AND THE GOVERNANCE OF THE INVISIBLE

Dr Tim Stevens, King's College London, UK

Accepted for publication in special issue of *International Politics*, on global prohibition regimes (2018).

ABSTRACT

This article explores the non-emergence of a global governance regime for cyberweapons. Cyberweapons are malicious software entities deployed to cause harm to adversaries' computer networks and systems. They threaten the integrity and functionality of digital systems that enable global circuits of communication and exchange, with significant potential impacts on social, economic and political order. Using a power-analytical approach, this article identifies four areas in which power works to constrain regime formation: the productive power of NATO's Tallinn Manual Process; the structural power of US involvement in cyberweapons markets; the institutional power of Internet technologies; and diplomatic claims to sovereignty that mask the operations of compulsory power. These work together to prevent a unified global approach to the regulation of cyberweapons. The article concludes that there are substantial obstacles to effective cyberweapons governance but that these should not prevent ongoing efforts to tackle this important and ubiquitous security issue.

KEYWORDS

cybersecurity; cyberweapons; global governance; security governance; global prohibition regimes; nonregimes

INTRODUCTION

It is over two decades since RAND analysts John Arquilla and David Ronfeldt established 'cyberwar' as a key concept in military thinking on information technology (Arquilla & Ronfeldt, 1993). Their original formulation of cyberwar as a mode of network-enabled military warfighting has been obscured by the term's subsequent translation and frequent misapprehension (Kaiser, 2015). Today, cyberwar is more likely to refer to a global state of *sub rosa* 'cyber skirmishing' and online crime, or to large-scale attacks on national critical infrastructures (Libicki, 2009, 2012; Betz and Stevens, 2011, p. 97), than a military engagement, such is the attenuation of its conceptualisation (see also, Arquilla, 2016, pp. viii-ix). However, militaries have embraced the promise that networked information technologies would restore the decisive advantage in war. They have become 'smart' or 'cybered' (Demchak, 2011), in military jargon, yet have frequently found themselves embroiled in relatively lo-tech expeditionary campaigns in which cognitive space has been as important as cyberspace (Betz, 2006; Lindsay, 2013a). Notwithstanding the persistence of the fog of war, modern militaries are now equipped to fight wars 'according to information-related principles' (Arquilla and Ronfeldt, 1993, p. 146) that maximize knowledge of the battlespace using hi-tech sensor-to-shooter systems and networked C5ISR (command, control, communication, computers, cyber, intelligence, surveillance, reconnaissance), in an attempt to tip the balance in their favour. This has become so normalised that military cyberwar is effectively just 'war' (Betz and Stevens, 2011; Whetham, 2016, pp. 85-87), although there exist within this distinct modalities of cyberwar*fare.*

Militaries – and their counterparts in the intelligence community – have also developed new tools for exploiting, subverting, degrading and destroying adversaries' informational assets, a category of capabilities loosely described as 'cyberweapons'. Rid and McBurney define

cyberweapons as ‘computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings’ (Rid and McBurney, 2012, p. 7; Rid, 2013, p. 37). This definition respects the established understanding of a weapon as ‘an offensive capability that is applied, or that is intended or designed to be applied, to an adversary to cause death, injury or damage’ (Boothby, 2016, p. 166).

The best-known example of a cyberweapon is malware (malicious software) known as Stuxnet, exposed in 2010 as a joint US-Israel project to sabotage the Iranian nuclear program (Sanger, 2012, pp. 188-225; Zetter, 2014). Once introduced to the internal computer networks of the Natanz nuclear facility by unknown human agents, Stuxnet sought out industrial software applications running on the Windows proprietary operating system. It then subverted the operations of equipment controlling nuclear centrifuges used for uranium enrichment, whilst masking its own presence and providing false information to internal monitoring systems. The process reportedly resulted in substantial physical damage to the centrifuge array, with the assumption that Stuxnet was therefore successful in its intention to set back Iran’s nuclear program. This assessment has been subject to some dispute (Barzashka, 2013; Slayton, 2016) but Stuxnet is widely regarded as the first known example of a state-sponsored cyberweapon being deployed in peace-time against a strategic adversary, although no perpetrators have yet to admit officially to their involvement. Even if it cannot claim to have retarded Iranian nuclear enrichment decisively, Stuxnet may have been effective in damaging Iranian confidence in its own security (Libicki, 2011, pp. 142-143) and some deterrent value may therefore have been derived from its use (Lindsay, 2013b; Lupovici, 2016). It stands in the security imagination as a watershed in the use of cyberweapons for political effect and a possible harbinger of the character of future inter-

state conflict (Farwell and Rohozinski, 2011, 2012; Collins and McCombie, 2012). More than sixty countries are reputed to be developing offensive cyber capabilities that might plausibly be considered cyberweapons (Valentino-Devries and Yadron, 2015).

The operational potential of cyberweapons has yet to be demonstrated fully to the public. They surely cannot yet reduce a targeted polity to 'Stone-Age technology' (Glenny, 2012, p. 245) but their continued development and use suggests they are important to the military and intelligence operations of any number of countries and non-state actors with access to the relevant technical capabilities (Gady, 2017). So too does the policy and academic attention given to their possible regulation since the late 1990s, which has produced a series of sensible proposals to limit or prohibit their development and use (Denning, 2000, 2001; Sofaer and Goodman, 2000; Rathmell, 2003; Prunkun, 2008; Ford, 2010; Geers, 2010; Meyer, 2011; Arimatsu, 2012; Wilson, 2013; Dunn Cavelty, 2014; Singer and Friedman, 2014, pp. 156-162). These analyses have concentrated on obstacles to regime formation, of which four are especially pertinent and recurrent: the absence of a consensus on norms of development, possession and use; the physical nature of cyberweapons and the digital environment; market disincentives; and, great power relations.

As of 2017, there is no international agreement on if or how cyberweapons should be regulated, nor is any formal overarching regime to do so imminent. Where the politics of this impasse are considered in previous work it is generally in the context of national interests or great power relations, principally those involving the US, Russia and China, that influence the cyberweapons debate in several important ways. However, there are limited discussions of cyberweapons that explore the operations of power beyond its conventional understanding as a mode of coercion and at scales other than the national or geopolitical. This article

addresses nascent attempts to regulate cyberweapons and explores the operations of power in the global information-technological assemblage that shape their development, possession and use. Specifically, it pursues a power-analytical reading of cyberweapons governance that hopes to better understand the regulatory effects of power within this field of security. Given the absence of a unified multilateral cyberweapons regime, this presents an opportunity to explore further how power operates to both facilitate and constrain the emergence of such a regime.

This article pursues a plural conceptualisation of power as the manifold relationalities of power that constitute and manifest in security regimes. Power is not a given attribute of an actor or agent but becomes apparent through its effects on others, often through their resistance to a given action or set of actions. It emerges through social relations, *sensu* Latour's (2005) sociomaterial theorisation of relations of the social, not merely from a conventional substrate of aggregate material capabilities. Social relations are, in one dimension – that of how power is expressed – either interactive or constitutive. In the second – regarding the specificity of the social relations of power – relations are direct and immediate, or indirect and diffuse. Mapped orthogonally, four categories of power can be identified: productive, structural, institutional and compulsory, which are described in detail elsewhere (Barnett and Duvall, 2005a, 2005b; Hynek, this volume). Productive power exists as the production of social actors through diffuse yet constitutive discursive and epistemic relations. Structural power works through the direct and mutual constitution of actors that determines their capacities, particularly through the production and reproduction of power hierarchies. Institutional power is evident in the indirect control or influence by one actor over the behaviours and conditions of existence of a socially distant other. Compulsory power also speaks to agent interactions but operates through direct rather than diffuse relations.

These four modalities of power correspond to the four principal obstacles to regime formation outlined above and structure the remainder of this article. The first section explores the role of the NATO Tallinn Manual Process in constructing cyberweapons as legitimate military instruments. This acts as a locus of epistemic authority that permeates NATO members' policy and doctrine on cyberwarfare and shapes key actors' subjectivities in hegemonic fashion, which prompts resistance from NATO's strategic adversaries. Section two identifies the role of US structural power in incentivising cyberweapons markets, which undermines multilateral attempts to regulate dual-use technologies associated with cyberweapons. The third section looks at the Internet as a source of institutional power. It argues that the design of the Internet provides affordances for cyberweapons, a situation at odds with the desires of the US, in particular, as the creator of the global Internet. This represents an ontological delimiting of hegemonic authority. The final empirical section addresses the diplomatic relations of the great powers, which resolve to differing interpretations of sovereignty and further constrain the emergence of a global cyberweapons regime. The article concludes by describing the manifold operations of power in the round and enquires after the prospects for global cyberweapons governance.

PRODUCTIVE POWER AND THE TALLINN MANUAL PROCESS

Rid and McBurney's analysis of cyberweapons recognises that 'identifying something as a weapon means, at least in principle, that it may be outlawed and its development, possession, or use may be punishable' (Rid and McBurney, 2012, p. 11). This suggests that cyberweapons might be suitable objects of global regulation or prohibition, practical difficulties in implementing such a regime notwithstanding. This focus on the regulatory or prohibitive outcomes of constructing software as weaponised code is understandable but

elides equally important aspects of cyberweapons discourse. Conferring weapons status on software is a means of legitimation as much as a mode of disciplinarity and constraint. For militaries and intelligence agencies, the entry of cyberweapons into policy and doctrine facilitates the use of cyberweapons, not their abandonment. The principal locus for developing norms around cyberweapons continues to be the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia. This became operational in 2008 as a formal International Military Organization (IMO) under NATO auspices and provides support to NATO and its member states on a range of cybersecurity and cyber defence issues. Contrary to popular belief, it was not founded in response to the politically motivated cyber attacks on Estonia in spring 2007, a series of events dubbed 'the first real war in cyberspace' (Landler and Markoff, 2007). The Centre had been approved in 2006 but the subsequent cyber attacks helped promote Estonia and the CCD COE in particular as key loci of technical capability and epistemic authority on cyber issues (Hansen and Nissenbaum, 2009).

At the heart of CCD COE activities is the Tallinn Manual Process (hereafter, TMP), an ongoing legal analysis of the applicability of international law to cyber conflict. This led to the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013).[1] The consensus emerging from the TMP's International Group of Experts is that the law of armed conflict and international humanitarian law do apply to cyberwarfare and, as such, cyberwarfare should be bound by the same legal frameworks that apply to other forms of military force. The TMP is not legally binding but the findings articulated in the *Tallinn Manual* have been incorporated rapidly into defence policy, strategy and doctrine. State parties like the UK and US affirmed the principles of the first volume in legal advice

[1] A second volume on international law and cyber operations that do not reach the threshold of war (Schmitt, 2017) was not published in time to be considered in this article.

(Koh, 2012) and in defence strategy (Ministry of Defence, 2013; US Department of Defense, 2015a). US military doctrine also respects TMP *opinio juris* on matters of cyberwarfare (US Department of Defense, 2015b), and NATO adopted TMP principles into its Enhanced Cyber Defence Policy (NATO, 2014, article 72) and Cyber Defence Pledge of July 2016 (NATO, 2016).

Rule 41 of the *Tallin Manual* defines cyberweapons and cyberweapons systems as 'cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack' (Schmitt, 2013, p. 119). The cyberweapon is that part of the cyberweapons system 'used to cause damage or destruction to objects or injury or death to persons' (Schmitt, 2013, p. 119). Additionally, use of cyberweapons must respect conventional norms of *jus in bello* and meet criteria of military necessity, proportionality and discrimination. Stuxnet is singled out in this regard as an example of a carefully planned operation against a discrete target, with due attention paid to minimising collateral damage (Schmitt, 2013, p. 141). States are obliged to consider the likely effects of military cyber operations ahead of deployment and to terminate them if they do not meet these criteria. This concern with weapons effects, rather than cyberweapons *per se*, is a consistent feature of the TMP and guides current US Department of Defense and State Department discussions on cyberweapons use (McGhee, 2016; Pomerleau, 2017). It is also consistent with historical targeting procedures of US military and intelligence with respect to cyber operations (Hayden, 2016, pp. 146-147).

In the absence of clear-cut precedents, how cyberwarfare and international law articulate will continue to develop through legal analysis and operational adaptation. The principal author of

the *Tallinn Manual* conceded that the TMP might change little, except, crucially, 'improved adherence to the rule of law in cyberspace' (Maher, 2013). It is in this normative sense, however, that the TMP is both a powerful agent of change and an expression of wider geopolitical issues that hinder the formation of a global regime for cyberweapons. In the first instance, the TMP 'produces reality … domains of objects and rituals of truth' (Foucault 1995, p. 194). This is a reality in which software and hardware combine to form cyberweapons systems with the capacity to cause harm analogous to an armed attack. It produces these informational objects as weapons, which therefore renders them normalised within military discourse and practice and as valid objects of legal sanction within the existing framework of customary international law. The aim of the TMP is not prohibition (Nadelmann, 1990) but facilitation of state use of cyberweapons. There is no suggestion that cyberweapons should be banned, except, perhaps, if used in specific categories of offensive action against civilians and civilian infrastructures (Barrett, 2013; Simpson, 2014). The intention is to provide a legal basis for the use of cyberweapons in war, so as to maintain and even maximise states' liberties of movement and action in global information environments. A regime governing weapons use and the conduct of war is already in place and efforts are therefore directed towards establishing its applicability to cyberwarfare and cyberweapons. The translation of TMP's principles and legal opinion into supranational (NATO) and national legal frameworks, policy, military doctrine and strategy, provides militaries with the 'rules of the game'. These allow them to always be 'playing to the edge' (Hayden, 2016) of the legal box circumscribing the use of cyberweapons in war.

The TMP also aids the formation of differentiated subjectivities contingent on actors' perceived attitudes to international law. The operational modes and means of cyberwarfare are deemed legitimate when used by states acting in compliance with the laws of war and

international humanitarian law. Countries that do not adhere to these norms must be deemed illegitimate, a list that, from a NATO perspective, inevitably includes Russia, China, Iran and North Korea, all of which have demonstrated proficiency and intent in the use of offensive cyber capabilities (Singer and Friedman, 2014; Segal, 2016) and without due regard for *jus cogens*. It also includes the use of cyberweapons by non-state actors, which is *a priori* illegitimate and fuels fears of 'cyberterrorism', a broad category of action for which little empirical evidence exists (Conway, 2011; Jarvis *et al*, 2014; Jarvis and Macdonald, 2015). The attempted fixing of subjectivities is, however, contested, particularly by Russia, which sees in the TMP evidence of a hegemonic thrust serving US interests (Krutskikh and Streltsov, 2014, p. 75). The US perceives that Russia and China disapprove of the TMP because it would make their own use of cyberweapons a matter of international legal attention (von Heinegg, 2015; Painter, 2016). This is a further expression of a longstanding disagreement between 'West' and 'East' over issues of Internet governance and state use of cyberspace (Stevens, 2012).

The TMP as a system of power-knowledge is centred on Estonia and the CCD COE and initially materialised in the artefact of the *Tallinn Manual* itself. Its translation into a range of NATO members' policy and doctrine demonstrates its mobility through the assemblages of military cooperation, standardisation and interoperability and its consequent rematerialisation in a wide range of institutional and informational forms. Cyberweapons are produced and legitimised as a weapons class through these discursive moves and reproduced via further mediations and wider political discourses. The aim of this process is to demonstrate that cyberweapons belong in the modern military arsenal and to define where the boundaries of their potentialities lie. This can only be achieved by asserting that international law applies to cyberweapons and that it provides for their permissive regulation. If it did not, either new

laws would be required, or cyberweapons would have to be abandoned, or they could only be used illegally; none of these options is attractive to NATO and its members. The productive power of the TMP serves to strengthen norms around cyberweapons use in war but also reifies and entrenches disagreements over those norms between NATO and its principal strategic adversaries.

STRUCTURAL POWER AND CYBERWEAPONS MARKETS

Any discussion of US leadership of NATO and its effects on international order must also be situated within considerations of its structural power in the global political economy. The US is the unquestioned leader in information-technological development and its cyberwarfare capabilities grant it a unique position in cyberweapons research and innovation. The Trump administration has indicated its willingness to accelerate the development and deployment of cyberweapons, which in turn may facilitate a cyber 'arms race' and destabilise international relations (Gady, 2017). There already exist robust cyberweapons markets of varying degrees of legality, particularly in 'zero-days', an essential component of any cyberweapon. Zero-days may be used in both defensive and offensive contexts and are an essential facet of cybersecurity research. Dorothy Denning, an early supporter of 'cyber arms controls', states explicitly that global prohibition of cyberweapons is neither desirable nor possible (Denning, 2001). One key reason is that prohibition of cyberweapons – or their zero-day components – would inhibit cybersecurity research and lead to greater insecurity in the global information environment. This argument has resurfaced since 2013, when the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods (1996) was extended to various classes of software and hardware 'specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software"' (Granick, 2014). The

debate over this revision shows how the US' structural power serves to undermine the regulation of cyberweapons.

Cyberweapons consist of three components, the absence of any one of which denies the categorisation of malware as a weapon proper: propagation method, payload and exploits (Herr, 2014). The propagation method defines how the code is delivered into a target system and the payload is the core executable code of the malware that determines its functionality and delivers its effects. The third component, the exploit, allows both propagation and payload delivery by taking advantage of vulnerabilities in computer systems and their defensive measures. Most software is demonstrably insecure in this context, either through failure to conform with security standards or as a result of code transcription and other errors in programming. 'There is no forced entry in cyberspace', writes Martin Libicki, 'If a destructive message gets into a system, it must be entirely across pathways that permit such a message to get through' (Libicki, 2007, pp. 35). Pathways may be human vectors, the targets of 'social engineering' (Abraham and Chengular-Smith, 2010), but most are 'bugs' in proprietary software and systems that inadvertently allow code to be infiltrated through any defensive measures that may be present.

Software bugs are usually unknown to system programmers, operators and users until they are exploited for the purposes of malware insertion. These vulnerabilities are often referred to as 'zero-day' ('0-day') vulnerabilities, indicating the time available to devise and deploy measures mitigating the possible or actual damage caused by their exploitation. 'Zero-day exploits' are malware written specifically to take advantage of undisclosed zero-day vulnerabilities before responsible parties can issue and apply 'patches' to rectify coding errors. This temporal advantage means that zero-day exploits are 'the most powerful attack

available to offensive cyber units' (Carr, 2010, p. 152). Stuxnet's use of at least four zero-day exploits indicates to many analysts the necessary involvement of at least one state party in its development, given the substantial resources required to identify any zero-day vulnerabilities, let alone several (Langner, 2011).

Zero-day vulnerabilities and exploits are of tactical and operational value but have significant financial value too. They are a highly desirable commodity and markets have evolved to satisfy demand for them. These have developed within the framework of a significant growth in markets for hacking tools, services and data obtained from cybercrime (Kshetri, 2010; Ablon *et al*, 2014). Zero-day markets trade in vulnerabilities and exploits, the relative proportion of which differs according to whether a market is characterised as white, grey, or black (Libicki *et al*, 2015, p. 44). In white markets, vulnerabilities are sold to software vendors offering 'bug bounties', so that vulnerabilities can be addressed before damage occurs. In this context, zero-days are not cyberweapons, as only vulnerabilities are traded, not exploits, and there is no intent to harm. Grey market actors are often government agencies or contractors that purchase vulnerabilities and exploits short of weaponisation (pseudo-exploits). These can be used either for state-sanctioned offensive purposes, or to improve defensive measures. One grey market instrument is the Vulnerabilities Equities Process of the US National Security Agency (NSA), which decides what to do when vulnerabilities are brought to the attention of the NSA (Schneier, 2015). The NSA claims it discloses vulnerabilities to software vendors so they may be patched, but activists accuse it of holding back vulnerabilities for intelligence and offensive cyberwarfare purposes, thereby putting software and its dependent services at unnecessary risk (Crocker, 2015).

Black zero-day markets are geared to cybercriminal purposes and trade in exploits and their associated vulnerabilities. These are inaccessible to ordinary users as they are in the so-called Dark Web, part of the World Wide Web that is not indexed by conventional search engines. Additionally, portions of the Dark Web exist on top of 'darknets', networks that can only be accessed using specific software installations and network configurations (Rid and Moore, 2016). These are peer-to-peer networks that hide, encrypt or anonymise Internet traffic, therefore making it difficult for investigators to establish user identity and location or the content of their communications. There are few academic studies of zero-day black markets but researchers and journalists indicate that increased recognition of their existence is accompanied by a rise in users' suspicion of external intervention, not least by government agents – who are sometimes also buyers – and greater premiums on discretion and 'knowing the right people' to facilitate trustworthy transactions (Egelman *et al*, 2013; Ablon *et al*, 2014, pp. 25-28; Tsyrklevich, 2015; Zetter, 2015).

Empirical data on cyberweapons prices and trade volumes are hard to obtain. Market researchers tend to over-value cyberweapons markets by several orders of magnitude, as they conflate cyberweapons with other information security products and services, notably anti-virus software. Estimates of $522 billion in 2021 (Transparency Market Research, 2015) and $4 trillion by 2024 (Market Info Group, 2013) are therefore heavily skewed towards legal markets in cybersecurity goods and services that do not qualify as cyberweapons in the sense intended here. An alternative indicator of market values is provided by unit costs for particular types of exploit, which range from a few thousand dollars to tens, even hundreds, of thousands of dollars, depending on the software targeted, the severity and longevity of a vulnerability, the sophistication of the exploit, and the disposition and identity of the buyer (Ablon *et al*, 2014, p. 26). In November 2015, security company Zerodium – 'We pay big

bounties, not bug bounties' – claimed to have paid hackers a 'seven-figure sum' for an exploit targeting Apple iPhones and iPads (Greenberg, 2015). Zerodium, like many other companies, counts governments amongst its clients. Zero-day markets therefore display a range of incentives, rewards, and dynamics of supply and demand, and are subject to a range of ethical constraints and actor motivations (Miller, 2007; Egelman *et al*, 2013).

The revised Wassenaar Arrangement was the first multilateral attempt to incorporate technology associated with cyberweapons into an international regime, although it stopped short of controls on intrusion software itself, in which category tools like zero-day exploits fall. The UK was a key driver of the amendment, keen to deflect domestic and international condemnation of British firms supplying surveillance technologies to authoritarian regimes, a category also covered by the revised Wassenaar Arrangement (Omanovic, 2015). The European Union and member-states like the UK implemented the new rules in relatively unproblematic fashion at the end of 2014 (Tung, 2014; Department for Business, Innovation and Skills, 2015). In the US, however, implementation foundered on the key issue of its impact on legitimate cybersecurity research (Blue, 2015; Pyetranker, 2015).The principal objection is that Wassenaar exposes all cyberweapons research to potential criminalisation if it falls foul of export controls. At the same time, the US is the main purchaser of exploits, which incentivises the market and makes it unlikely to abstain from transactions it sees as beneficial to its national and economic security.

Cyberweapons markets are supported by robust consumer demand, both state and non-state, and there are no obvious alternative goods and services, factors that act against their successful prohibition (Nadelmann, 1990, p. 486). Without firm US support, their regulation via mechanisms like the Wassenaar Arrangement is unlikely to achieve its desired effect,

although, in common with other arms export control regimes, it may have some longer-term utility in promoting multilateral norms on dual-use technology transfer (Pyetranker, 2015). However, US structural power as the dominant producer and consumer of cyberweapons components and research disincentivises market regulation and encourages international trade in code entities like zero-day exploits.

INSTITUTIONAL POWER AND THE INTERNET

The issue of cyberweapons falls under the rubric of cybersecurity as broadly understood. It is well-established there is no global regime for cybersecurity governance and a significant literature exists querying why this is and how to remedy this situation (e.g. Hughes, 2010; Sofaer *et al*, 2010; Stevens, 2012; Mueller *et al*, 2013; Hurwitz, 2014; Nye, 2014). This mirrors the wider milieu of Internet governance, which has long rejected the possibility of holistic governance of such a complex and extensive entity in favour of identifying which aspects of the Internet require what forms of governance (DeNardis, 2014, p. 226; Mueller, 2010). This has led to the emergence of a 'regime complex' of 'loosely coupled sets of regimes' (Keohane and Victor, 2011, p. 7) for governing specific forms of activity in and through the Internet (Nye, 2014). This includes regimes and institutions with dedicated responsibilities for core Internet governance issues like technical policies and standards, and those with jurisdictions that originate outside Internet governance but overlap with it, such as telecommunications, finance, trade, intellectual property, and national security. So diverse is this regulatory and sociotechnical landscape that it seems 'unlikely that there will be a single overarching regime for cyberspace any time soon' (Nye, 2014, p. 13; Hurwitz, 2014). Indeed, the 'multistakeholder' model has become the dominant template for managing global Internet governance (Carr, 2015).

This focus on regimes and institutions has shown how institutional power operates in the international system to promote and contest forms of cybersecurity governance. As we have seen, various institutions are engaged in aspects of cyberweapons governance also, such as NATO, the CCD COE and the Wassenaar Arrangement. What is missing from most of these accounts is a consideration of the institutional power of the Internet itself (DeNardis, 2012, 2014). Like all infrastructures, the Internet is the product of social action and embedded within it are the outcomes of decisions and contestations that shape social behaviours and 'present a formidable set of real constraints on the realm of the possible' (Deibert, 2003, p. 530; Aradau, 2010). McCarthy explicitly frames the Internet as a 'technological institution', which by 'including and excluding certain practices the Internet prevents and promotes goals in line with the goals of its designers' (McCarthy, 2015, p. 67). The design decisions, norms of use, even technical standards, of the Internet thereby instantiate the institutional power of major actors in this technological space. As the originator of the Internet architecture and the rules that govern its functionality, US hegemony is therefore supported by the institutional power of the Internet (McCarthy, 2015, p. 68). In many respects this is demonstrable, but cyberweapons require that we amend and our understanding of the institutional power of the Internet. Specifically, how do cyberweapons challenge the supposed alignment of design goals and political intent implied by this model of institutional power?

The original design decision of the Internet is that it was built with little concern for security, prioritising instead the ease and speed of communication between geographically distant nodes like universities and defence establishments (Eriksson and Giacomello, 2007, p. 6). Since its inception in the 1960s, the Internet has evolved to become the most remarkable and ubiquitous technology of its age, but it remains insecure and prone to exploitation and subversion (Barnard-Wills and Ashenden, 2012). This is not to say that it is easy to do so but

that it may be so compromised by actors with the requisite technical skills and malicious intent. Revisiting the thesis that there is 'no forced entry in cyberspace' (Libicki, 2007, p. 35) provides us with an opportunity to examine cyberweapons in the context of institutional power. Cyberweapons do not break through defences like a battering ram but are more like a stiletto blade inserted between the ribs (Stone, 2013, p. 106). In this analogy, the soft skin and tissue between the ribs offers the potential for the insertion of the stiletto – it is an affordance, understood as an opportunity for action embedded in the environment.[2] Affordances may or may not be recognised by an actor but they are there, 'a property of both the environment and the perceiving organism, and where in that interaction opportunity for action lies' (Taylor, 2012, p. 8).

Cyberweapons do not perceive their environment in an animal sense but they are programmed to seek out affordances (vulnerabilities) and exploit them for payload delivery (Herr, 2014). Once inside a target system, they can manipulate its conditions of existence and functionality. At the 'smart' end of the spectrum, cyberweapons act as 'intelligent agents' that access specific systems, evaluate these environments, and act autonomously to achieve particular goals (Rid and McBurney, 2012, p. 9; also, Valeriano and Maness, 2014, pp. 353-355). The affordances that provide cyberweapons with their action opportunities may arise from deficiencies in design processes ('the Internet was built for simplicity not security'), or from the emergent properties of complex systems ('we didn't expect that'). In the former situation, the policy answer is to promote better cybersecurity, to reduce the 'attack surface' of information systems, and to invest in cyber defences both active and passive. In the latter case, the picture is more complicated. It may be that it is impossible to design software and information systems that do not provide affordances for malware. Formal verification of

[2] I am indebted to Samuel Forsythe for this insight.

software security has long been a goal of software engineers (Mackenzie and Pottinger, 1997) and an elusive one at that. It was only in 2016 that programmes like the DARPA-funded High-Assurance Cyber Military Systems project have suggested that perfect software security might be attainable but this is a long way from network-level deployment (Hartnett, 2016). Even were this possible, it would still not mitigate human error. Cyberweapons systems cannot be understood only as combinations of software and hardware but as assemblages also incorporating human actors (Danks and Danks, 2016). Weapons are always hybrid assemblages of non-human and human entities (Latour, 1994; Bourne, 2012), which within themselves also offer affordances for action.

This picture is complicated further because cyberweapons have no conventional physical form. They are software, 'information objects' that lack corporeality but whose existence, operations and effects necessarily involve physical processes, entities and events (Dipert, 2014, pp. 36-37). This property alone sets cyberweapons apart from most other weapons classes, the majority of which possess identifiable material forms of payload and delivery system. Cyberweapons are 'latent', in that they are 'in the world but not experienced as part of the world' (Floridi, 2014, p. 318), until their effects manifest in more conventionally apprehensible fashion. This is an important consideration, as their immateriality complicates their practical identification and interdiction, and also because all existing legal regimes recognise weapons as material entities (Mele, 2013, p. 9; Jenkins, 2013). Like the conflicts of which they are a part, cyberweapons 'require special interfaces to be perceived [and] a special sensitivity to be eradicated' (Floridi, 2014, p. 319). The invisibility of digital affordances presents a daunting challenge in this respect.

These observations offer an important corrective to the view that the institutional power of the Internet inevitably supports the hegemonic interests of the United States. We might argue that cyberweapons exploit vulnerabilities caused in part by the very technological institution created by the US in the first place. This is not a question of blame but it does suggest that the institutional power of the Internet can work against the interests of even those actors whose structural and productive power is most evident. In 1991, when the term 'electronic Pearl Harbor' was coined, its progenitor Winn Schwartau drew special attention to the vulnerability of a 'processing-intensive society' like the US (Schwartau, 1991). The implication over the last quarter-century has been that the US is *uniquely vulnerable* to informational attacks. This impression has been attenuated somewhat as the Internet has spread globally but the ontological condition of insecurity is perhaps felt most acutely by those countries in which Internet penetration is the greatest and, further, illustrates the limits of US hegemony. The institutional power of the Internet will continue to promote the utility of cyberweapons until such time as the technological institution itself can be organised and built differently.

COMPULSORY POWER AND DIPLOMACY

The operations of compulsory power form the last modality of power considered here. Under specific consideration is how the diplomatic actions and motives of the great powers – US, Russia, China – prevent policy coordination and the formation of a global regulatory or prohibition regime for cyberweapons. In the previous discussion of productive power and the Tallinn Manual Process, we alluded to the existence of a diplomatic standoff between the US and Russia/China on matters of Internet governance and state use of cyberspace. This disagreement colours the discussion of cyberweapons regulation irrevocably and is rooted in national conceptions of the applicability of sovereignty to the global information environment. What results is an impasse that delivers little diplomatic progress towards a

binding regime whilst allowing for the continued development and operational deployment of cyberweapons.

The debate about sovereignty and the Internet is two decades old and remains unresolved. Indeed, it has become one of the central features of international policy and diplomacy on Internet-related issues, particularly Internet governance, which must surely be considered a mature domain of global policy. The same perhaps cannot be said of cyberwarfare, although the Tallinn Manual Process and various national initiatives stemming from it have at least advanced an understanding of cyberwarfare as amenable to regulation under customary international law. In either field, however, sovereignty remains the central concept, the contestation of which is inhibiting more expansive regulatory regimes. As with any form of international policy coordination and cooperation, the primary consideration for states is 'how much' sovereignty must be 'given up' in order to achieve collective ends. In the example of the Council of Europe Convention on Cybercrime, for example, which is open for ratification by any state, neither Russia nor China will sign on account of fears that the transnational police coordination the Convention requires would violate their national sovereignty and security and is consequently a price not worth paying (Clough, 2014). Both countries prefer instead the forum of the regional Shanghai Cooperation Organization (SCO) for discussion and resolution of cybercrime issues (Dalla Guarda, 2015).

The reasons for this surface also in their rejection of the Tallinn Manual Process, in which several different forms of sovereignty are at play. As Betz and Stevens (2011, pp. 55-74) assess, not all forms of sovereignty are affected equally by the Internet. International legal sovereignty is barely affected, as the Internet does not impact states' sovereign equality in international law. Conversely, transnational data flows pose a major challenge to

interdependence sovereignty and the ability of states to control these cross-border flows. When ideas are transmitted across national borders they can also pose a threat to domestic sovereignty. When malware does, it violates Westphalian sovereignty and the principle of non-interference in domestic affairs. China and Russia's concerns prioritise domestic and interdependence sovereignty and the deleterious effects of externally-generated information on domestic security and regime stability. Moreover, both China and Russia, in common cause with other authoritarian regimes, promote 'Internet sovereignty' or 'cyber sovereignty' as a means of reinforcing domestic control and authority (Nocetti, 2015; Zeng *et al*, 2017). This is visible in a range of repressive measures aimed at curtailing freedom of speech and expression online and the influx of subversive ideas across their territorial borders (Deibert and Crete-Nishihata, 2012). It is also the driver behind Sino-Russian proposals for multilateral information security agreements that would enshrine these prerogatives in law (Dalla Guarda, 2015, pp. 223-236). Information security is not a technical prospect in these proposals but a process of controlling ideas and information within sovereign borders.

The rejection of the Tallinn Manual Process speaks to this situation in various ways. The US is attempting to apply existing international law to cyberwarfare and cyberweapons and rejects calls for an international treaty, whilst promoting global norms for state uses of cyberspace. It does this to preserve its freedom of movement in foreign territories and networks within the framework of international law. Russia and China are seeking an international treaty that would cover cyberwarfare, in order to preserve their freedom of action at home. Through a process of 'forum shopping' (Murphy and Kellow, 2013), China and Russia have settled on the SCO and the UN's International Telecommunications Union (ITU) as the appropriate venues for promoting this project. The former is the principal strategic counterpart to NATO and *de jure* excludes the United States. The US in turn holds

the ITU in as low regard as Russia and China do the CCD COE in Tallinn. Each 'side' in this competitive process to win other states' support considers its own fora as the proper loci of relevant epistemic and moral authority. Neither side is disposed to shift from its diplomatic position. In the meantime, the cyber activities of all three countries undermine their pretensions to moral leadership. Stuxnet exposed American use of offensive cyber capabilities and Edward Snowden disclosed the global surveillance activities of US intelligence agencies (Greenwald, 2014). These same agencies have confidently identified Russia as responsible for attempts to influence the 2016 presidential election through cyber means (ODNI, 2017). China's record of political cyber surveillance and state-sponsored commercial cyberespionage has been the object of significant global attention for many years (Lindsay *et al*, 2015).

The persistent violation of Westphalian sovereignty these actions represent is rapidly becoming the 'cyber new normalcy' (Korns, 2009). Received wisdom is that cyberspace favours offence over defence (e.g. Lynn, 2010), and cyberweapons are perceived as necessary means to restore the decisive advantage promised by early visions of cyberwar and informationalised warfare in general, as well as integral components of intelligence machineries. Specifically, cyberweapons are viewed as agents of compulsory power in and of themselves, with great potential for coercion in times of war and peace. This renders the use of cyberweapons an increasingly attractive proposition for states capable of developing or purchasing them. Several authors note that the offence-defence balance is not as radically destabilised by cyberweapons as is commonly supposed (Rid, 2013; Lindsay, 2013b, 2014) but there is good reason to be alert to a developing 'cult of the offensive' amongst policy-makers, military leaders and intelligence officials (Slayton, 2016, p. 73). Significantly, this would suggest an emerging cyber 'arms race', supported by a burgeoning cyber military-

industrial complex (Deibert, 2011). This is precisely the sort of situation that might eventually require an international treaty or arms control mechanism, which would throw the international community back upon all the problems of maintaining such a regime, given inherent difficulties in monitoring, verification and enforcement.

OUTLOOK

Weapons can be understood as 'the violent materiality of the existential condition of uncertainty' (Booth and Wheeler, 2008, p. 42). We may query whether cyberweapons are either violent or material but they do express and shape a condition of marked uncertainty in the contemporary international order. Silent, invisible and potentially very effective, they are attractive to states and non-state actors seeking advantage in war and in peace, a distinction blurred by just such tools as these. Physical attributes aside, they would seem to be suitable targets for regulation or prohibition, given the transnational nature of the problem and the lack of ability to deal with them on a national level (Nadelmann, 1990). Yet no unitary or global regime has emerged to regulate them. Indeed, the circulation of mutually corroborating powers outlined in the preceding account suggests that the barriers to regime formation are substantial. It might therefore be supposed that cyberweapons – or offensive cyber capabilities if we prefer – consist presently on the global level as 'a transnational policy issue area characterized by the absence of multilateral institutions for ordering actors' interactions', that is, as a 'nonregime' (Dimitrov *et al*, 2007, p. 234). The central question, then, is how can a power-analytical approach to cyberweapons inform our understanding of this nonregime?

Nonregimes may in time evolve into regimes but a range of factors inhibit this process. Cyberweapons governance is hampered by the nature of the digital environment, which affords multiple vulnerabilities that can be exploited by malicious actors. Their

unconventional physical nature also complicates potential identification and interdiction. Understood as a form of institutional power, Internet technologies prevent ready solutions to the problem of weaponised code, as well as creating significant friction for hegemonic aspirations for the Internet. However, states continue to desire and develop cyberweapons because of their perceived military and intelligence utility in the projection of compulsory power. This is despite those countries with the most developed cyber capabilities being perhaps those with most to lose by their use, given their socioeconomic hyperconnectivity. Particularly in the case of the US, its influence in the global malware marketplace represents a powerful instance of structural power, given how it disincentivises other actors both state and non-state. The general willingness of capable states to use offensive cyber capabilities further undermines attempts to generate global norms about cyberweapons use. The Tallinn Manual Process is an important node in western productive power but it seeks not to prohibit cyberweapons but to facilitate their use. In this respect, it puts cyberweapons on a legal footing equivalent to other weapons classes. Given the technological pre-eminence of the USA, it also serves to reproduce the power structures that enable American dominance in the first place. Unsurprisingly, this hegemonic ambition is challenged in diplomatic fora by the other great powers, which play the game of compulsory power through various means. They too, of course, seek to shape global norms through their own productive and institutional power, even if their ambitions differ from those of the US. Together, this manifold of powers prevents regime formation at the global level.

It may be that states are not yet convinced of the need to regulate cyberweapons. Certainly, we have not yet seen sufficient evidence of their promised capabilities to engage the public imagination or to engender moral entrepreneurship on the issue (Nadelmann, 1990). There is also little political appetite for dispensing with these tools, which means that decisive

political will supporting prohibition is unlikely. The emphasis thus far has been on regulation, in keeping with other weapons classes, although these attempts are partial and contested. From a global governance perspective, however, analytical attention on prospective formal institutionalisation of norms and practices at the truly global level is perhaps misleading. All existing work on cyberweapons regulation and governance presents barriers to regime formation without recognising that global regimes are never perfect. They are all, in some sense, fragmented (Biermann *et al*, 2009), and fragmentation itself should not be viewed as terminally problematic. In the case of cyberweapons, the Tallinn Manual Process and Wassenaar Arrangement are significant steps towards a global governance architecture (Stevens, 2017). It should also be remembered that many potential uses of cyberweapons constitute crimes in most jurisdictions, and transnational regimes are developing in cybercrime policy.

The sociotechnical environment through and over which cyberweapons governance would be expected to operate 'has never been more in flux' (Deibert, 2015, p. 15). Cyberwarfare and cyberweapons hit the front pages in 2016, taking centre-stage in a range of geopolitical conflict, particularly between the US and Russia. We may take issue with calling code a 'weapon' but there is no doubt that states and other actors are using offensive cyber capabilities with growing confidence and relative impunity. If we perceive that regulation of these tools is necessary and socially beneficial, then the processes outlined above will have to be addressed as matters of urgency. Attention to the operations of power in this strategic, political and technological environment indicates some specific issues that will require concerted efforts if the nonregime is to transition into a regime.

ABOUT THE AUTHOR

Tim Stevens is Lecturer in Global Security in the Department of War Studies, King's College London. His work has appeared in the journals, *Contemporary Security Policy*, *International Political Sociology*, *Security Dialogue* and *Politics & Policy*. He is the co-author of *Cyberspace and the State* (Routledge, 2011) and his latest book is *Cyber Security and the Politics of Time* (Cambridge University Press, 2016).

REFERENCES

Ablon, L., Libicki, M.C. and Golay, A.A. (2014) *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: RAND Corporation. Research report.

Abraham, S. and Chengalur-Smith, I. (2010) An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society* 32(3): 183-196.

Aradau, C. (2010) Security that matters: Critical infrastructure and objects of protection. *Security Dialogue* 41(5): 491-514.

Arimatsu, L. (2012) A treaty for governing cyber-weapons: Potential benefits and practical limitations. In: C. Czosseck, R. Ottis and K. Ziolkowski (eds.) *Proceedings of the 4th International Conference on Cyber Conflict; 5-8 June, Tallinn, Estonia*. Tallinn: NATO CCD COE Publications, pp. 91-109.

Arquilla, J. (2016) Foreword: Ethics for the coming epoch of conflict. In: F. Allhoff, A. Henschke and B.J. Strawser (eds.) *Binary Bullets: The Ethics of Cyberwarfare*. New York: Oxford University Press, pp. vii-xii.

Arquilla, J. and Ronfeldt, D. (1993) Cyberwar is coming! *Comparative Strategy* 12(2): 141-165.

Barnard-Wills, D. and Ashenden, D. (2012) Securing virtual space: cyber war, cyber terror, and risk. *Space & Culture* 15(2): 110-123.

Barnett M. and Duvall R. (2005a) Power in global governance. In: M. Barnett and R. Duvall (eds.) *Power in Global Governance*. Cambridge: Cambridge University Press, pp. 1-32.

Barnett, M. and Duvall, R. (2005b) Power in international politics. *International Organization* 59(1): 39-75.

Barrett, E.T. (2013) Warfare in a new domain: the ethics of military cyber-operations. *Journal of Military Ethics* 12(1): 4-17.

Barzashka, I. (2013) Are cyber-weapons effective? *The RUSI Journal* 158(2): 48-56.

Betz, D.J. (2006) The more you know, the less you understand: the problem with information warfare. *Journal of Strategic Studies* 29(3): 505-533.

Betz. D.J. and Stevens, T. (2011) *Cyberspace and the State*. London: Routledge.

Biermann, F., Pattberg, P., van Asselt, H. and Zelli, F. (2009) The fragmentation of global governance architecture: a framework for analysis. *Global Environmental Politics* 9(4): 14-40.

Blue, V. (2015) Weaponizing code: America's quest to control the exploit market. *Engadget*, 29 May, http://uk.engadget.com/2015/05/29/weaponizing-code/, accessed 18 February 2017.

Booth, K. and N.J. Wheeler (2008) *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. Basingstoke: Palgrave Macmillan.

Boothby, B. (2016) Cyber weapons: Oxymoron or a real world phenomenon to be regulated? In: K. Friis and J. Ringsmose (eds.) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Abingdon: Routledge, pp. 165-174.

Bourne, M. (2012) Guns don't kill people, cyborgs do: a Latourian provocation for transformatory arms control and disarmament. *Global Change, Peace & Security* 24(1): 141-163.

Carr, J. (2010) *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly.

Carr, M. (2015) Power plays in Internet governance. *Millennium: Journal of International Studies* 43(2): 640-659.

Clough, J. (2014) A world of difference: the Budapest *Convention on Cybercrime* and the challenges of harmonisation. *Monash University Law Review* 40(3): 698-736.

Collins, S. and McCombie, S. (2012) Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism* 7(1): 80-91.

Conway, M. (2011) Against cyberterrorism. *Communications of the ACM* 54(2): 26-28.

Dalla Guarda, N. (2015) Governing the ungovernable: International relations, transnational cybercrime law, and the post-Westphalian regulatory state. *Transnational Legal Theory* 6(1): 211-249.

Danks, D. and Danks, J.H. (2016) Beyond machines: Humans in cyberoperations, espionage, and conflict. In: F. Allhoff, A. Henschke and B.J. Strawser (eds.) *Binary Bullets: The Ethics of Cyberwarfare*. New York: Oxford University Press, pp. 177-197.

Deibert, R.J. (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium: Journal of International Studies* 32(3): 501-530.

Deibert, R.J. (2011) Tracking the emerging arms race in cyberspace. *Bulletin of the Atomic Scientists* 67(1): 1-8.

Deibert, R.J. (2015) The geopolitics of cyberspace after Snowden. *Current History* 114(768): 9-15.

Deibert, R.J. and Crete-Nishihata, M. (2012) Global governance and the spread of cyberspace controls. *Global Governance* 18(3): 339-361.

Demchak, C.C. (2011) *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA and London: University of Georgia Press.

DeNardis, L. (2012) Hidden levers of Internet control: an infrastructure-based theory of Internet governance. *Information, Communication & Society* 15(5): 720-738.

DeNardis, L. (2014) *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Denning, D. (2000) Reflections on cyberweapons controls. *Computer Security Journal* 16(4): 43-53.

Denning, D. (2001) Obstacles and options for cyber arms control. Paper presented at the Arms Control in Cyberspace conference; 29-30 June, Berlin.

Department for Business, Innovation and Skills (2015), Intrusion software tools and export control. August, http://blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf, accessed 18 February 2017.

Dimitrov, R.S, Sprinz, D.F., DiGiusto, G.M. and Kelle A. (2007) International nonregimes: a research agenda. *International Studies Review* 9(2): 230-258.

Dipert, R. (2014) The essential features of an ontology for cyberwarfare. In: P.A. Yannakogeorgos and A.B. Lowther (eds.) *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton, FL: Taylor and Francis, pp. 35-48.

Dunn Cavelty, M. (2014) Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics* 20(3): 701-715.

Egelman, S., Herley, C. and van Oorschot, P.C. (2013) Markets for zero-day exploits: Ethics and implications. In: *Proceedings of the 2013 New Security Paradigms Workshop; 9-12 September, Banff, Canada*. New York: Association for Computing Machinery, pp. 41-46.

Eriksson, J. and Giacomello, G. (2007) Introduction: Closing the gap between international relations theory and studies of digital-age security. In: J. Eriksson and G. Giacomello (eds.) *International Relations and Security in the Digital Age*. London and New York: Routledge, pp. 1-28.

Farwell, J.P. and Rohozinski, R. (2011) Stuxnet and the future of cyber war. *Survival* 53(1): 23-40.

Farwell, J.P. and Rohozinski, R. (2012) The new reality of cyber war. *Survival* 54(4): 107-120.

Floridi (2014) The latent nature of global information warfare. *Philosophy & Technology* 27(3): 317-319.

Ford, C.A. (2010) The trouble with cyber arms control. *The New Atlantis* 29(4): 52-67

Foucault, M. (1995) [1975] *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Gady, F-S. (2017) Trump and offensive cyber warfare. *The Diplomat*, 16 January, http://thediplomat.com/2017/01/trump-and-offensive-cyber-warfare/, accessed 12 February 2017.

Geers, K. (2010) Cyber weapons convention. *Computer Law and Security Review* 26(5): 547-551.

Glenny, M. (2012) *Dark Market: How Hackers Became the New Mafia*. London: Vintage.

Granick, J. (2014) Changes to export control arrangement apply to computer exploits and more. The Center for Internet and Society, Stanford Law School, 15 January, https://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more, accessed 18 February 2017.

Greenberg, A. (2015) Hackers claim million-dollar bounty for iOS zero day attack', Wired, 2 November, http://www.wired.com/2015/11/hackers-claim-million-dollar-bounty-for-ios-attack/, accessed 18 February 2017.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. London: Hamish Hamilton.

Hansen, L. and Nissenbaum, H. (2009) Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53(4): 1155-1175.

Hartnett, K. (2016) Hacker-proof code confirmed. *Quanta Magazine*, 20 September, https://www.quantamagazine.org/20160920-formal-verification-creates-hacker-proof-code/, accessed 16 February 2017.

Hayden, M.V. (2016) *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press.

Herr, T. (2014) *PrEP: A Framework for Malware and Cyber Weapons*. Washington, DC: George Washington University Cyber Security Policy and Research Institute. Report GW-CSPRI-2014-2.

Hughes, R. (2010) A treaty for cyberspace. *International Affairs* 86(2): 523-541.

Hurwitz, R. (2014) The play of states: Norms and security in cyberspace. *American Foreign Policy Interests* 36(5): 322-331.

Jarvis, L. and Macdonald, S. (2015) What is cyberterrorism? Findings from a survey of researchers. *Terrorism and Political Violence* 27(4): 657-678.

Jarvis, L., Macdonald S. and Nouri, L. (2014) The cyberterrorism threat: Findings from a survey of researchers. *Studies in Conflict and Terrorism* 37(1): 68-90.

Jenkins, R. (2013) Is Stuxnet physical? Does it matter? *Journal of Military Ethics* 12(1): 68-79.

Kaiser, R. (2015) The birth of cyberwar. *Political Geography* 46: 11-20.

Keohane, R.O. and Victor D.G. (2011) The regime complex for climate change. *Perspectives on Politics* 9(1): 7-23.

Koh, H.H. (2012) International law in cyberspace. Speech to USCYBERCOM Inter-Agency Legal Conference. Fort Meade, MD, 18 September.

Korns, S.W. (2009) Cyber operations: the new balance. *Joint Forces Quarterly* 54(3): 97-102.

Krutskikh, A. and Streltsov, A. (2014) International law and the problem of international information security. *International Affairs [Mezdunarodnaia zhizn]* 60(6): 64-76.

Kshetri, N. (2010) *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* Berlin: Springer.

Landler, M. and Markoff, J. (2007) In Estonia, what may be the first war in cyberspace. *The New York Times*, 28 May.

Langner, R. (2011) Cracking Stuxnet, a 21st-century cyber weapon. Speech to TED2011 Conference. Long Beach, CA, 3 March.

Latour, B. (1994) On technical mediation – Philosophy, sociology, genealogy. *Common Knowledge* 3(2): 29-64.

Latour, B. (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Libicki, M.C. (2007) *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.

Libicki, M.C. (2009) Sub rosa cyber war. In: C. Czosseck and K. Geers (eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, pp. 53-65.

Libicki, M.C. (2011) Cyberwar as a confidence game. *Strategic Studies Quarterly* 5(1): 132-146.

Libicki, M.C. (2012) The specter of non-obvious warfare. *Strategic Studies Quarterly* 6(3): 88-101.

Lindsay, J.R. (2013a) Reinventing the revolution: Technological visions, counterinsurgency criticism, and the rise of special operations. *Journal of Strategic Studies* 36(3): 422-453.

Lindsay, J.R. (2013b) Stuxnet and the limits of cyber warfare. *Security Studies* 22(3): 365-404.

Lindsay, J.R. (2014) The impact of China on cybersecurity: Fiction and friction. *International Security* 39(3): 7-47.

Lindsay, J.R., Cheung T.M. and Reveron, D.S., eds. (2015) *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press.

Lupovici, A. (2016) The 'attribution problem' and the social construction of 'violence': Taking cyber deterrence literature a step forward. *International Studies Perspectives* 17(3): 322-342.

Lynn, W.J. (2010) Defending a new domain: the Pentagon's cyberstrategy. *Foreign Affairs* 89(5): 97-108.

McCarthy, D.R. (2015) *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet*. Basingstoke: Palgrave Macmillan.

McGhee, J.E. (2016) Liberating cyber offense. *Strategic Studies Quarterly* 10(4): 46-63.

MacKenzie, D. and Pottinger, K. (1997) Mathematics, technology, and trust: Formal verification, computer security, and the US military. *IEEE Annals of the History of Computing* 19(3): 41-59.

Maher, H. (2013) New manual explains laws of cyberwarfare. Radio Free Europe / Radio Liberty, 1 April, http://www.rferl.org/content/new-manual-rules-cyberwarfare/24944686.html, accessed 18 February 2017.

Market Info Group (2013) *Cyber Weapons (Offensive and Defensive) for Government and Private Sectors: Global Market and Technologies Forecast, 2026*. Colorado Spring, CO: Market Info Group. Market report.

Mele, S. (2013) *Cyber-Weapons: Legal and Strategic Aspects*, version 2.0. Rome: Italian Institute of Strategic Studies.

Meyer, P. (2011) Cyber-security through arms control: an approach to international co-operation. *The RUSI Journal* 156(2): 22-27.

Miller, C. (2007) *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*. Baltimore, MD: Independent Security Evaluators. Research report.

Ministry of Defence (2013) *Cyber Primer*. London: Ministry of Defence.

Mueller, M.L. (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Mueller, M., Schmidt, A. and Kuerbis, B. (2013) Internet security and networked governance in international relations. *International Studies Review* 15(1): 86-104.

Murphy, H. and Kellow, A. (2013) Forum shopping in global governance: Understanding states, business and NGOs in multiple arenas. *Global Policy* 4(2): 139-149.

Nadelmann, E.A. (1990) Global prohibition regimes: the evolution of norms in international society. *International Organization* 44(4): 479-526.

NATO (2014) Wales Summit Declaration. Press release, 5 September, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, accessed 15 February 2017.

NATO (2016) Cyber Defence Pledge. Press release, 8 July, http://www.nato.int/cps/en/natohq/official_texts_133177.htm, accessed 15 February 2017.

Nocetti, J. (2015) Contest and conquest: Russia and global internet governance. *International Affairs* 91(1): 111-130.

Nye, J.S., Jr. (2014) *The Regime Complex for Managing Global Cyber Activities*. Waterloo, ON: Centre for International Governance Innovation, and London: Royal Institution for International Affairs, Chatham House. Global Commission on Internet Governance Paper Series no. 1.

Office of the Director of National Intelligence (ODNI) (2017) *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment, 6 January, https://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html, accessed 18 February 2017.

Omanovic, E. (2015) US publishes proposed rules implementing 2013 Wassenaar Agreements. Privacy International, 28 May, https://www.privacyinternational.org/?q=node/588, accessed 18 February 2017.

Painter, C.M.E. (2016) Testimony of Christopher M.E. Painter, Coordinator for Cyber Issues, US Department of State, Before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy. Hearing on 'International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms', 25 May, http://www.foreign.senate.gov/imo/media/doc/052516_Painter_Testimony.pdf, accessed 15 February 2017.

Pomerleau, M. (2017) How the Pentagon is shaping cyber tool use. *C4ISRNet*, 9 January, http://www.c4isrnet.com/articles/authorities-complicate-the-use-of-cyber-capabilities, accessed 15 February 2017.

Prunkun, H. (2008) 'Bogies in the wire': Is there a need for legislative control of cyber weapons? *Global Crime* 9(3): 262-272.

Pyetranker, I. (2015) An umbrella in a hurricane: Cyber technology and the December 2013 Amendment to the Wassenaar Arrangement. *Northwestern Journal of Technology and Intellectual Property* 13(2): 153-180.

Rathmell, A. (2003) Controlling computer network operations. *Studies in Conflict and Terrorism* 26(3): 215-232.

Rid, T. (2013) *Cyber War Will Not Take Place*. London: Hurst & Company.

Rid, T. and McBurney, P. (2012) Cyber-weapons. *The RUSI Journal* 157(1): 6-13.

Rid, T. and Moore, D. (2016) Cryptopolitik and the darknet. *Survival* 57(1): 7-38.

Sanger, D.E. (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers.

Schmitt, M.N., ed. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, M.N., ed. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Schneier, B. (2015) Hacking Team, computer vulnerabilities, and the NSA. *Schneier on Security*, 15 September, https://www.schneier.com/blog/archives/2015/09/hacking_team_co.html, accessed 18 February 2015.

Schwartau, W. (1991) Fighting terminal terrorism. *Computerworld*, 28 January, p. 23.

Segal, A. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs.

Simpson, T.W. (2014) The wrong in cyberattacks In: L. Floridi and M. Taddeo (eds.) *The Ethics of Information Warfare*. London: Springer, pp. 141-154.

Singer, P.W. and Friedman A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Slayton, R. (2016) What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security* 41(3): 72-109.

Sofaer, A.D., Clark, D. and Diffie, W. (2010) Cyber security and international agreements. In: *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy; 10-11 June, Washington, DC*. Washington, DC: The National Academies Press, pp. 179-206.

Sofaer, A.D. and Goodman, S.E. (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*. Stanford, CA: Stanford University. Working paper.

Stevens, T. (2012) A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy* 33(1): 148-170.

Stevens, T. (2017) Cyberweapons: an emerging global governance architecture. *Palgrave Communications* 3, DOI: 10.1057/palcomms.2016.102.

Stone, J. (2013) Cyber war *will* take place! *Journal of Strategic Studies* 36(1): 101-108.

Taylor, M. (2012) Terrorism and affordance: an introduction. In: M. Taylor and P.M. Currie (eds.) *Terrorism and Affordance*. London and New York: Continuum, pp. 1-17.

Transparency Market Research (2015) *Cyber Weapon Market: Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2015-2021*. Albany, NY: Transparency Market Research. Market report.

Tsyrklevich, V. (2015) Hacking Team: a zero-day market case study. 22 July, https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/, accessed 18 February 2017.

Tung, L. (2014) EU exploit vendors will need a 'licence to sell' from 31 December. *CSO Online*, 19 December, http://www.cso.com.au/article/562845/eu-exploit-vendors-will-need-licence-sell-from-31-december, accessed 18 February 2017.

US Department of Defense (2015a) *Cyber Strategy*. Washington, DC: Department of Defense.

US Department of Defense (2015b) *Law of War Manual*. Washington, DC: Office of General Counsel, Department of Defense.

Valentino-Devries, J. and Yadron, D. (2015) Cataloging the world's cyberforces. *The Wall Street Journal*, 11 October, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710, accessed 15 February 2017.

Valeriano, B. and Maness, R.C. (2014) The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research* 51(3): 347-360.

Von Heinegg, W.H. (2014) *International Law and International Information Security: A Response to Krutskikh and Streltsov*. Tallin Paper 9. Tallinn: CCD COE Publications.

Whetham, D. (2016) Cyber *chevauchées*: Cyberwar can happen. In: F. Allhoff, A. Henschke and B.J. Strawser (eds.) *Binary Bullets: The Ethics of Cyberwarfare*. New York: Oxford University Press, pp. 75-88.

Wilson, C. (2013) Cybersecurity and cyber weapons: Is nonproliferation possible? In: M. Martellini (ed.) *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*. Heidelberg: Springer, pp. 11-24.

Zeng, J., Stevens, T. and Chen, Y. (2017) China's solution to global cyber governance: Unpacking the domestic discourse of 'Internet sovereignty'. *Politics & Policy* 45(3): 432-464.

Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

Zetter, K. (2015) How the secretive market for zero-day exploits works. *Slate*, 24 July, http://www.slate.com/blogs/future_tense/2015/07/24/new_insights_into_zero_day_exploit_sales.html, accessed 18 February 2017.